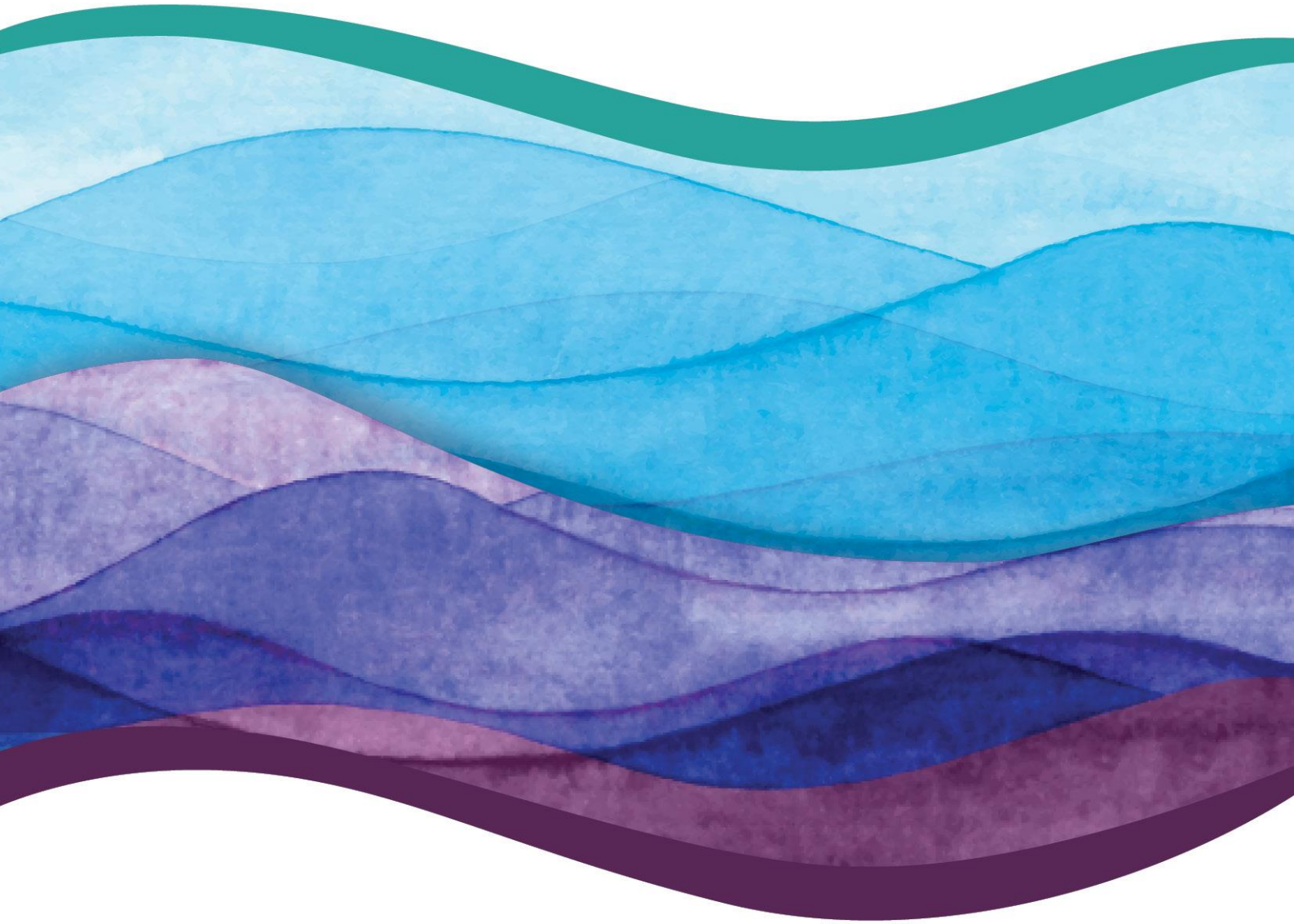
Domestic and Family Violence Information Sharing Guidelines

Practical guidance



Women's Safety and Justice Reform

Queensland Government

Table of Contents

Practical guidance and tips

This document is intended to complement the Domestic and Family Violence Information Sharing Guidelines (the Guidelines) and provide further guidance on the application of the information sharing provisions in the *Domestic and Family Violence Protection Act 2012* (DFVP Act).

The Guidelines should be used as the main point of reference, with this document used to provide additional practical guidance and tips.

While every effort has been made to provide accurate and helpful information, this document does not constitute legal advice and users should seek their own independent legal advice in relation to their statutory and legal obligations.

Understanding the intent of the information sharing provisions

The overarching intent of the information sharing provisions in Part 5A of the DFVP Act is to enable certain entities to share information on a confidential basis that helps them to work together to prevent and reduce the risk of domestic and family violence (DFV) threats.

Entities may determine they need to share information for many reasons, including:

- To contribute to a holistic view of the risk of DFV for assessment purposes.
- To benefit from the expertise of another entity during risk assessment or collaborative safety planning.
- Because the specific response needs of the victim-survivor are more aligned with the scope and expertise of the other entity.
- Because it is safer for the other entity to respond to the threat.

Whatever the reason for sharing the information, it is important for entities to remember that the information sharing provisions exist because entities have different skills, experience, scope, legislative powers, and expertise that contribute to a holistic response to DFV threats.

In addition to adhering to the information use provisions of Part 5A, entities should:

- **Respect the expertise of the entity they are sharing information with**
  The receiving entity is included in the information sharing provisions for a reason. The sharing entity will not be sharing the information if they do not believe that it would prevent or reduce the risk from DFV.
- **Participate in collaborative decision making and safety planning with regards to the use of shared information**
  The entity sharing the information, and the entity receiving the information, should work in a collaborative and consultative manner regarding the use of the information. The victim-survivor's self-determination should be respected at each stage of the process, and their best interests should be front and centre in every decision to share, or not share, information.
- **Consider other perspectives**
  The differing expertise and skills across entities is what makes integrated responses to DFV effective. Differences of opinion and perspective should be approached in a collaborative and consultative way, to achieve the best outcome for the person experiencing violence.

Understanding differing views on information sharing

The information sharing provisions rely on practitioners and others to use their professional judgement to make a decision about whether and how information should be shared. Each person's professional

judgement will be influenced by their own personal experiences and knowledge of DFV and of the entity they represent. Each situation is approached from multiple unique perspectives.

It is important that information sharing is approached in a collegial way, and not in an adversarial way. The information sharing provisions are not a mechanism for shifting risk or responsibility, or a reporting mechanism. Best practice information sharing includes shared responsibility for risk management and support.

Where decisions are made with the underlying intent of the information sharing provisions in mind (that is, whether sharing the information will help to maximise the victim-survivor's safety, health, and wellbeing), staff can trust and respect the decisions of others, even if they may not agree.

When consent for sharing information cannot be obtained, practitioners and others are faced with the challenge of balancing a victim-survivor's wishes with obligations to act on known information. Staff that work directly with victim-survivors are acutely aware that they have been entrusted with highly personal information and that victim-survivors have a right to expect that this will be kept in confidence and only used for appropriate purposes. Staff may also be subject to internal policies and processes that, while aligning with the information sharing provisions, are not always clear to, or well understood by, others.

In understanding others' decisions around information sharing, it can be helpful to know more about the person's role in assessing and responding to DFV, the remit of the entity they represent, and limits imposed on the entity. Open lines of communication are essential. Working closely with other agencies and organisations in the local integrated service response can help to build strong working relationships built on trust and mutual respect.

Cultural considerations when sharing information

Respecting the cultural protocols of the victim-survivor and promoting cultural safety should be of critical importance when disclosing or using information about First Nations peoples or culturally and linguistically diverse communities. The Common Risk and Safety Framework (CRASF) provides further guidance on engaging with First Nations victim-survivors and victim-survivors from culturally and linguistically diverse backgrounds.

Delivering culturally safe services requires creating an environment which recognises and respects a person's cultural identity. It is important that practitioners and others are aware of the many factors that influence a person's experience of DFV and consider any cultural factors and potential implications which may impact on the sharing of information.

For First Nations peoples, this can include:

- consideration of the impact of colonisation, discrimination, and intergenerational trauma on First Nations peoples and how this contributes to a distrust of government and hesitancy to share information
- consideration of the victim-survivor's community and familial connections and relevant confidentiality issues when sharing information with First Nations services who may know the victim-survivor or person using violence (PuV)
- clearly communicating to the victim-survivor that only relevant information will be shared and how it will be used
- reassuring the victim-survivor about how privacy and confidentiality will be ensured once information is shared
- considering the differing family kinships and definitions of 'family violence' that exist in First Nations communities

- reflecting on and addressing any unconscious bias or assumptions when engaging with the victim-survivor or PuV.

For people from other culturally and linguistically diverse communities, consideration should be given to:

- how a victim-survivor's migration or residency status may contribute to their hesitancy to share information and make them vulnerable to certain forms of DFV
- how DFV and consent may be understood differently across different cultures
- the victim-survivor's level of understanding about the Australian justice system
- ensuring culturally appropriate supports have been offered to the victim-survivor, including an interpreter or translator where appropriate
- clearly communicating to the victim-survivor that only relevant information will be shared and how it will be used
- reassuring the victim-survivor about how privacy and confidentiality will be ensured once information is shared.

Considerations when sharing within a small community

Where a population is relatively small and connected, including in urban areas, entities should consider how community links can impact on the confidentiality and privacy of victim-survivors. For example, the local police officer or support worker may know a victim-survivor and/or the PuV.

To help protect the safety and confidentiality of the victim-survivor, it is important that only relevant information is shared, and only when sharing the information would help to keep the victim-survivor safe through the assessment of, or response to, the DFV risk. Professional judgement should be used, with consideration to:

- the connections that the victim-survivor or PuV may have with staff at local services
- ensuring any requests for information are genuine and not made by someone with a conflict of interest toward the victim-survivor or PuV
- additional safety planning to manage any risk posed from sharing information.

Sharing the information of children and young people

The DFVP Act recognises that children and young people can be particularly vulnerable to DFV and makes provisions for their protection, including through information sharing, where appropriate. There are, however, some things to consider when sharing information about a child or young person.

Wherever safe, possible, and practical, a person's consent should be obtained before sharing their information. Children and young people should also be offered the opportunity to provide consent, where it is safe, possible, and practicable to do so. The Office of the Information Commissioner Queensland advises that as far as possible, especially for older children, children should be given the opportunity to make decisions about their rights and how agencies deal with their personal information.[i]

Whether a child or young person under the age of 18 can give informed consent must be determined on a case-by-case basis. The child or young person must have capacity to give consent, meaning that they have sufficient understanding and maturity to understand what is being proposed.

Importantly, parental consent to share information about the child or young person is not a necessity. In some cases, it may be appropriate to seek the consent of the non-offending parent, however, extreme

[i] https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/applying-the-privacy-principles/privacy-and-children

caution should be taken to ensure that this does not inadvertently place the child or young person at greater risk. **Parental consent from the PuV should never be sought.**

If consent is sought and obtained from a child or young person, the entity should keep comprehensive and contemporaneous records (e.g. file notes) of any consultations with the child or young person and the reasons why the entity considers the child has capacity to consent.

If a child or young person gives consent but the non-offending parent does not (or vice versa), each factual situation should be carefully considered before the entity discloses the information.

Where consent from a child or young person is not given or cannot be obtained, information may be shared without consent in line with the provisions at Part 5A.

The Common Risk and Safety Framework provides further guidance on engaging with children and young people.

Using appropriate and non-judgemental language

When sharing information, practitioners and others should ensure that language used is succinct, includes only relevant information and is non-judgemental. Language should validate and emphasise the victim-survivor's strengths and place the responsibility for the abuse entirely with the PuV.

It's important to note that these records may also be subpoenaed and should be recorded clearly and appropriately. Information shared can be factual or opinion, but opinions shared should relate to professional judgement regarding the likelihood and severity of the threat.

Considerations when sharing information about a victim-survivor's location

It is important that steps are taken by entities to mitigate the risk of a PuV locating a victim-survivor as a result of information sharing. This includes obscuring any identifying information relating to the victim-survivor's current location, and clearly including privacy and confidentiality disclaimers on all forms and files containing confidential domestic violence information.

Record keeping and storage of personal information

It is critical that information regarding a victim-survivor or the PuV is safely and securely stored by the receiving entity. One of the key reasons victim-survivors are hesitant to share information is out of fear of the PuV accessing the information and locating them or otherwise using it against them. It is important that steps are implemented to prevent personal information being accessed or disclosed. This can include using physical and electronic security measures (i.e. locks or swipe cards, passwords) or operational security measures (i.e. restricting access to relevant staff only).

Entities should record where an individual has provided consent (or not), what the individual provided consent for, and what the individual was advised about the future use or on-sharing of that information.

Entities should also have a process in place that allows for information received under Part 5A to be readily identified as information obtained under Part 5A and ensure that sufficient security measures are in place to:

a) prevent unauthorised access to that information; and

b) ensure that the information is only used for the purposes of assessing or responding to a DFV risk.

All entities, whether covered by the Information Privacy Principles, National Privacy Principles or other privacy legislation, must protect the information from misuse and should follow the appropriate information storage rules for their organisation. Refer to pp. 24-25 for further guidance on proper storage of information.

Sharing information about persons using violence and alleged persons using violence

The underlying intent of the information sharing provisions is to maximise the victim-survivor's safety, protection and wellbeing. The PuV's consent should not be sought as this could unintentionally place the victim-survivor at greater risk.

The criteria for sharing information (entity classification, practitioner's role, and usage) apply for information relating to both the victim-survivor and the PuV. Page 20 of the Guidelines outlines situations where information cannot be shared. If a practitioner or entity is unclear whether the limitations in s169J of the Part 5A provisions apply to them, they should seek legal advice.

Information sharing in the context of High Risk Teams

The information sharing provisions are not limited only to high-risk cases. The same provisions apply both within, and outside of, the High Risk Team (HRT).

Information is not 'owned' by any particular entity. Information sharing should not come from a position of whose information it is to share, but what information is available to support risk assessment and safety management.

Once an entity is in possession of information shared under Part 5A, that information can be used in a manner permitted by the information sharing provisions. That is, the information can only be used for the purpose of assessing or responding to a DFV threat. This may include providing relevant information to another staff member employed within that entity, as long as the on-sharing of the information falls within one of the permitted uses under the usage provisions.

Entities should take care to put in place measures that readily identify information received under Part 5A and ensure that sufficient security measures are in place to:

a) prevent unauthorised access to that information; and

b) ensure that the information is only used for the purposes of assessing or responding to DFV risk.

Utilising the expertise of specialists in domestic and family violence

Some employees may work within an entity that is classified as a specialist DFV service provider or prescribed entity and meet the practitioner's role requirements to share information under Part 5A, but not have experience and expertise in DFV that would qualify them as a 'DFV specialist'. While not a DFV specialist, they may still assess or respond to DFV threats as part of their role.

In these circumstances, it is best practice for the employee to liaise with other DFV specialists who work within their entity prior to sharing information under Part 5A.

Frequently Asked Questions

Understanding consent and guiding principles

Do Part 5A provisions only apply when sharing information without consent?

Part 5A provisions apply in any situation where information is shared to assess or manage DFV risk, regardless of whether the victim-survivor has provided consent or not. Even if a victim-survivor has consented to an entity sharing their information, the provisions in Part 5A apply regarding permitted uses, storage, and limits on sharing.

What if another entity refuses to share information with me?

Communication is key when negotiating information sharing between entities. An entity can request information from another entity but cannot compel the entity to share the information. The Part 5A provisions are enabling, not mandatory. An entity will make a decision based on professional judgement about whether sharing the information is likely to maximise the safety, protection, and wellbeing of the victim-survivor.

When requesting or sharing information, it is important to keep the underlying intent of the information sharing provisions and the principles for information sharing in mind. Where decisions are made with the underlying intent in mind (that is, whether sharing the information will help to maximise the victim-survivor's safety, health, and wellbeing), staff can trust and respect the decisions of others, even if they may not agree.

When sharing information under Part 5A, do I have to use a specific template?

There is no requirement for information shared under Part 5A to be included on a specific template or in a certain format. Some entities may promote the use of templates, however the intent of Part 5A is to enable swift action to promote the safety of a victim-survivor and this should not be delayed by excessive administrative burden.

Managing privacy and confidentiality

I have concerns that sharing information may inadvertently place the victim-survivor at greater risk. What should I do?

The underlying intent of the information sharing provisions (refer to p.6 of the Guidelines) should form the basis of decisions around whether or not information should be shared. The information sharing provisions *allow* an entity to share information, it does not *compel* a person to do so. If an entity believes that sharing information would help to keep the victim-survivor safe, then it may be appropriate to share the information. If sharing information would not help to keep the victim-survivor safe, it should not be shared.

Potential risks to the victim-survivor must always be considered prior to information being shared. An entity should take steps to mitigate any identified risks. The Guidelines provide guidance around considering the safety implications of sharing information on p.18.

When information is shared, it is good practice for both the 'sharer' and the 'receiver' of the information to liaise on the best course of action. No single entity is responsible for holding the risk associated with a case. Information is shared to support and inform integrated service responses to help keep the victim-survivor safe. Liaising on possible courses of action will support good decision making.

Can I share information about a child or young person under Part 5A?

There is nothing in the DFVP Act that prohibits information about children or young people from being shared under Part 5A. However, there are some things to consider when sharing information about a child or young

person. Refer to the Practical Guidance and Tips section on sharing the information of children and young people for further information.

Can information be shared in cases of adolescent to parent violence?

Yes. The information sharing provisions cover family relationships, which can include adolescent to parent relationships. For more information, refer to the Practical Guidance and Tips section on sharing the information of children and young people.

Can information about the person using violence be shared with a victim-survivor?

Sharing relevant information about the PuV may potentially increase the victim-survivor's safety. Relevant information may be shared with a victim-survivor to assist them to manage their safety or that of their children.

What about the person using violence's rights to privacy of information?

The underlying intent of the information sharing provisions is to maximise the victim-survivor's safety, protection, and wellbeing. The PuV's consent should not be sought as this could unintentionally place the victim-survivor at greater risk.

How many years back can information be shared?

The DFVP Act does not stipulate a limitation on time regarding the sharing of information. However, a practitioner should consider the relevance of information that is not current in the context of the purpose of sharing the information.

Guidance on when information cannot be shared is available on p.20 of the Guidelines.

Understanding terminology

What constitutes a 'serious threat'?

There is no set definition of serious threat in Part 5A, and no criteria or threshold that must be met before information is shared. Professional judgement is required to determine whether there is a sufficient risk to the victim-survivor that requires information sharing to maximise their safety, protection and wellbeing.

In determining whether a threat is 'serious', consider:

- A 'serious threat' need not (but may) be a threat to the life of the person. The threat could be to cause physical, emotional, or psychological harm.
- A 'serious threat' may be understood in terms of the severity of harm being threatened, or to the probability of that harm occurring.
- A threat should be of sufficient seriousness to give cause for apprehension.

The Common Risk and Safety Framework should be used when assessing the level of DFV risk and can provide further guidance on risk factors, means, capacity, and intent. If a CRASF Level 2 risk assessment is undertaken and indicates there is risk, this is likely a good indicator that the threat is serious.

Entity classifications, practitioner's role requirements and usage requirements

If I work in a specialist DFV service provider but my role is not in frontline service delivery, can I still share information under Part 5A provisions?

Working in a frontline position is not a requisite for information sharing. If you work in a specialist DFV service that receives government funding and your role requires you to assess threats to life, health or safety because of DFV or to take action to lessen or prevent threats to life, health or safety because of DFV by providing assistance or a service, you can share information.

A full definition of each entity classification is provided on pp. 10-11 and a flowchart on pp. 27-30 of the Guidelines.

I work for a sub-organisation that seems to fit a different classification than the head organisation, is this possible?

In situations where there is an umbrella organisation with multiple sub-organisations operating within it, it may be possible for the sub-organisation to have a different classification to the umbrella organisation. This will be dependent on the funding relationship and employment structure. The sub-organisation must receive government funding directly (as opposed to the head organisation) and must employ individuals directly (i.e. individuals are not all employed to the head organisation). This means that the information sharing requirements may be different between the sub-organisations.

I am not a practitioner. How can I be sure that my role meets the 'Practitioner's role' requirements? How do I determine whether an activity can be classified as either assessing or responding to a DFV threat?

In order to share, receive or use information under Part 5A, a person's duties must include assessing threats to life, health or safety because of DFV, or taking action to lessen or prevent threats to life, health or safety because of DFV.

This does not mean that you must be a specialist in DFV and you do not necessarily need to be in a frontline role. But it does mean that the requirement to assess or respond to DFV threats is a foreseeable requirement of the role. This could be a role where a person's experience of DFV may be disclosed to you in the course of your duties, for example counsellors, health practitioners, or some community service organisations.

If DFV is disclosed to you in the course of your duties and you are required to make a professional judgement about risk to a client, your role would likely be considered to include assessing DFV threats.

For a role to include *responding* to a DFV threat, some proactive step or intervention must be taken to address the threat. This could be as simple as making a referral to another service or contacting a specialist DFV service provider for advice.

As an example, a hairdresser may in the course of their duties have information disclosed to them that may lead them to suspect DFV is occurring. The hairdresser could screen for risk using the CRASF level 1 tool. This would constitute an assessment. However, the requirement to assess or respond to DFV threats is not a foreseeable requirement of a hairdresser's role. Therefore, the hairdresser **would not** meet the practitioner's role requirements.

Can an entity share information it has, but which does not directly relate to their usual scope of work?

Yes. Information sharing should not come from a position of whose information it is to share, but what information is available to support risk assessment and safety management. If an entity is in possession of information that may help to keep a victim-survivor safe, they can share that information in line with the provisions under Part 5A.

Why is a prescribed entity defined in Part 5A as the Chief Executive of a relevant Queensland Government department? Wouldn't the prescribed entity be the department? What impact does this have?

The inclusion of Chief Executive in the definition of a prescribed entity is not intended to have any practical impact on the sharing of information under Part 5A. The reference to a Chief Executive in this context does not suggest that there is a need for a person to be at an executive or other specific level in an entity to share information.

If a person employed by a prescribed entity meets the criteria set out under s169H of the Part 5A provisions then they are able to share, receive or use information on behalf of a Chief Executive of a prescribed entity.

I am a staff member employed in a prescribed entity. Am I automatically delegated authority by the Chief Executive to share information?

No. Being employed or engaged by a prescribed entity does not automatically assume you have been delegated authority to share information.

To share information on behalf of an entity you must meet the requirements set out in s169H of Part 5A, including:

- that your role within the organisation includes assessing or responding to DFV threats, or taking action to lessen or prevent threats to life, health or safety because of DFV; and
- the purpose for sharing information must be to assess or respond to a DFV threat.

If you do not meet the two criteria above, you may still be able to share information on behalf of an entity if you have received clear authority from that entity to do so. This could include delegation through internal policies or protocol that determine that you are authorised to receive, share, or use information under the Part 5A provisions.

I am a specialist DFV practitioner, but I am employed by a support service provider (not a specialist DFV service provider). Why am I not classified as a specialist DFV service provider?

An entity's classification applies to the entity as a whole, including all the individuals employed within it.

It may be possible in certain situations for an individual to be classified as a specialist DFV service provider. This will be dependent on the funding relationship. If the government funding is provided to an individual, then the specialist DFV service provider is the individual. If the funding is to an organisation, then the specialist DFV service provider is that organisation as a whole, not the individuals comprising it.

My entity receives government funding for generalist services, but many of the entity's clients are people experiencing DFV. Shouldn't we be considered a specialist DFV service provider?

Many organisations receive funding to provide services that someone experiencing DFV may access, however, this does not mean that your service would meet the specialist DFV service provider criteria.

Specialist DFV service providers are funded to provide DFV services specifically targeting people at risk of, experiencing, or using DFV. For instance, this may be funding for DFV counselling, or DFV court-based services. While a service could be funded for general counselling or wellbeing programs that a person at risk of, experiencing, or using DFV may use – it is not a DFV-specific services and is not necessarily targeted to this group.

A good way to see if your organisation may meet the specialist DFV service provider criteria is to consider if they are funded under the Domestic and Family Violence investment specifications. Most specialist DFV service providers will receive funding for service types under these specifications.

If an entity receives time-limited grant funding for a DFV project, does this classify the entity as a specialist DFV service provider?

To be classified as a specialist DFV service provider, an entity must receive government funding (may be State or Commonwealth funding) to provide DFV services to persons who fear or experience domestic violence, or who commit domestic violence. The funding does not necessarily need to be ongoing, but it must be for the delivery of a DFV *service,* Grant funding for a project or event is unlikely to meet the criteria of a DFV service. Once an entity ceases to receive government funding for the DFV service, they would cease to be classified as a specialist DFV service provider.

For more information on the definition of a specialist DFV service provider, including examples, refer to pp. 10, 11 of the DFV Information Sharing Guidelines. Managing information after it has been shared

Who owns the information once it has been shared? Can I share the information further?

No entity 'owns' the information. The information always remains the property of the victim-survivor.[ii] If an entity has *possession* of information, it may form a record of that entity.

Once an entity is in possession of information shared under Part 5A, that information can be used in a manner permitted by the information sharing provisions. That is, the information can only be used for the purpose of assessing or responding to a DFV threat. Entities should take care to put in place measures that readily identify information received under Part 5A and ensure that sufficient security measures are in place to:

a) prevent unauthorised access to that information; and

b) ensure that the information is only used for the purposes of assessing or responding to DFV risk.

Usual information storage and security requirements apply (refer to pp. 24-25 of the Guidelines for further information).

[ii] Note: Certain legislative restrictions may limit or prohibit the provision of court documents to the victim-survivor and other persons whose details are included in the documents.

Information sharing should not come from a position of whose information it is or whether the information relates specifically to the remit of the entity, but what information is available to support risk assessment and safety management. If an entity is in possession of information that may help to keep a victim-survivor safe, they can share that information in line with the provisions under Part 5A.

Can information shared under Part 5A be used for other purposes, such as to inform intake and assessment processes?

Use of information shared under Part 5A must align with the usage requirements outlined in Part 5A. That is, the information can only be used for the purpose of assessing or responding to a DFV threat. If the intended activity can be considered either assessing or responding to a DFV threat, then the information shared under Part 5A may be used.

Can information shared under Part 5A of the DFVP Act be subpoenaed or used in other court or justice processes?

Use of information shared under Part 5A must align with the usage requirements outlined in Part 5A, unless another law compels you to share that information. For instance, if an entity is seeking to use or share information received under Part 5A to support court documents for a purpose that is not assessing or responding to a DFV threat, then it would not be appropriate to use the information in this way.

However, if a court issues a subpoena for information that was shared with an entity under Part 5A, an entity may have to share the information as this would be a requirement under another law. In this circumstance, the information is no longer subject to Part 5A requirements, as it is being shared under other legislation.

It is important to remember that information on a shared database is considered to be within the possession of an entity that has access to the database. If an entity receives a subpoena for information, they should seek legal advice on how to respond before providing information.

If a person has any concerns about any information disclosed in a subpoena, these concerns should be raised at the time of the information being provided. It is important that the safety of the victim-survivor is forefront, and that relevant safety planning is undertaken to manage any risk posed by releasing the documents.

The way that information is recorded, including language, is important to ensure that a victim-survivor is not placed at further risk if the records are used in Court proceedings. Language should be non-judgemental and only include relevant information. Language should validate and emphasise the victim-survivor's strengths and place the responsibility for the abuse entirely with the PuV.

Information shared can be fact or opinion, but opinions shared should relate to professional judgement regarding the likelihood and severity of the threat.

Information sharing and High Risk Teams

Can information shared through the HRT be used outside of the HRT or after a case has been 'stepped down'?

The purpose of the provisions under Part 5A are to maximise the wellbeing, protection, and safety of victim-survivors and to assess and manage the risk from DFV. This applies across all levels of the DFV integrated service system – not only when cases are referred to HRT.

Information can continue to be shared in line with the requirements of Part 5A of the DFVP Act to assess and manage DFV risk when a case has been stepped down from an HRT.

Information shared at the HRT can also be used outside of the HRT as long as it aligns with the usage provisions outlined in Part 5A. That is, the information can only be used for the purpose of assessing or responding to a DFV threat.

This may include providing relevant information to another staff member employed within that entity, as long as the on-sharing of the information falls within one of the permitted uses under the usage provisions.

Entities should take care to put in place measures that readily identify information received under Part 5A and ensure that sufficient security measures are in place to:

a) prevent unauthorised access to that information; and

b) ensure that the information is only used for the purposes of assessing or responding to DFV risk.

Interaction with other legislation

Can I share information with Commonwealth or interstate entities?

Part 5A only enables information sharing within the Queensland jurisdiction. However, entities may share information with interstate or Commonwealth entities where it is permitted in under other laws, for example the *Privacy Act 1988* (Cth).

I am a mandatory reporter. If I receive information shared under Part 5A that creates a reasonable suspicion that a child is at risk of significant harm, do I still need to make a mandatory report even though the information does not 'belong' to my entity?

The information sharing provisions do not have any impact on mandatory reporting obligations. If a mandatory reporter is in possession of information that warrants a mandatory report to be made, they are obligated to do so, even if the information was shared under Part 5A.

It is also important to note that sharing information under Part 5A does not replace mandatory reporting obligations. Usual processes for making a mandatory report must be followed.

If information is shared with the Queensland Police Service (QPS) under Part 5A, is QPS required to investigate under s100? What does this involve?

A police officer is required to investigate under s100 of the DFVP Act if they 'reasonably suspect' that domestic violence has been committed. However, s169L(3) of the DFVP Act *prevents* a police officer from using information received under Part 5A for an investigation without first consulting with the entity who shared the information under Part 5A and considering whether the use of the information for the investigation would be in the best interests of the victim-survivor.

This requirement for consultation should never be treated perfunctorily or as a mere formality. Rather, a collaborative approach should be taken to support informed decision-making. While the police officer is not required to act in accordance with the sharing entity's advice, the obligation to consult does require the police officer to consider the sharing entity's views about the proposed use of the information.

The DFVP Act does not impose a positive obligation on a police officer to make direct contact with the PuV and/or victim-survivor as part of a DFV investigation under s100. Accordingly, if QPS is required to investigate under s100 and that investigation uses information shared under Part 5A, they can investigate without making the PuV aware of the investigation, suspicion, or complaint.

If the investigation leads the police officer to reasonably believe that domestic violence has been committed, the police officer must consider whether it is *necessary* or *desirable* to take further action to protect the victim-survivor from violence and whether *immediate* action is required to protect the victim-survivor from further violence.

When considering the necessity or desirability of the action to be taken, the police officer should consider the wellbeing and safety of the person experiencing violence, and unintended consequences of the action.

The DFVP Act provides that the officer *may* take the following action to protect the person from further violence:

- apply for a protection order, temporary protection order, variation of a DVO or issue a police protection notice
- take the respondent into custody
- take any other appropriate action in the circumstances.

Examples of other actions that may be appropriate include taking the respondent to another place, such as a hospital.

Section 100 **does not require** a police officer to take any **specific** action at the conclusion of the investigation, but does require them to consider the appropriate action to be taken in line with the general principle of the DFVP Act that protecting the victim-survivor's safety and wellbeing is paramount. In line with s169L(3)(b) of the DFVP Act, information would not be used in an investigation if it is deemed to not be in the best interests of the victim-survivor.

If, after the investigation, the police officer decides not to take any action, the police officer must make a written record of the police officer's reasons for not taking any action.

Find out more

Where can I find more resources and training regarding the Guidelines and Part 5A?

Further resources, including factsheets, targeted training modules and a decision tree can be found at http://www.qld.gov.au/dfvinformationsharingguidelines.